الأمن السيبراني و الشبكات

بحث شامل ومُمنهج عن **الامن السيبراني و الشبكات** Cybersecurity and Network يغطي المفاهيم الأساسية، العلاقة بين المجالين، وأبرز التحديات والتقنيات الحديثة.

1. شبكات الحاسوب (Computer Networks)

تُعرف شبكة الحاسوب بأنها نظام يربط بين جهازين أو أكثر لتبادل البيانات والموارد (مثل الإنترنت، الطابعات، والملفات). بناء شبكة آمنة هو الخطوة الأولى لحمايتها.

أ. أنواع الشبكات حسب النطاق الجغرافي

- **LAN (Local Area Network):** شبكة محلية تغطي مساحة صغيرة مثل منزل، مكتب، أو مدرسة.
- **WAN (Wide Area Network):** شبكة موسعة تربط بين مدن أو دول كاملة، والإنترنت هو أكبر مثال عليها.
- **WLAN (Wireless LAN):** الشبكة المحلية اللاسلكية (مثل شبكات Wi-Fi).

ب. النموذج المرجعي للاتصالات (OSI Model)

لفهم كيف تنتقل البيانات وكيف يتم تأمينها، يُقسم الاتصال إلى 7 طبقات في نموذج OSI، حيث تمثل كل طبقة وظيفة محددة:

١ **الطبقة الفيزيائية (Physical):** الأسلاك، كابلات الألياف الضوئية، والإشارات اللاسلكية.
٢ **طبقة ربط البيانات (Data Link):** تنظيم البيانات في "إطارات" (Frames) والتعرف على الأجهزة عبر عنوان MAC.
٣ **طبقة الشبكة (Network):** توجيه البيانات (Routing) عبر الحزم (Packets) باستخدام بروتوكول الإنترنت (IP).
٤ **طبقة النقل (Transport):** ضمان نقل البيانات بدقة عبر بروتوكولات مثل TCP و UDP.
٥ **طبقة الجلسة (Session):** إدارة وفتح وإغلاق جلسات الاتصال بين الأجهزة.
٦ **طبقة العرض (Presentation):** تشفير البيانات وتنسيقها (مثل تحويل البيانات إلى صيغ مفهومة).
٧ **طبقة التطبيق (Application):** الواجهة التي يتفاعل معها المستخدم (مثل بروتوكولات HTTP, FTP, SMTP).

2. الأمن السيبراني (Cybersecurity)

الأمن السيبراني هو ممارسة حماية الأنظمة، الشبكات، البرامج، والبيانات من الهجمات الرقمية. يرتكز الأمن السيبراني على ثلاثة أعمدة رئيسية تُعرف بـ **مثلث** (CIA Triad) **CIA**:

- **السرية (Confidentiality):** ضمان عدم وصول البيانات إلا للأشخاص المصرح لهم فقط (بواسطة التشفير وصلاحيات الوصول).
- **النزاهة/سلامة البيانات (Integrity):** حماية البيانات من التعديل أو الحذف غير المصرح به (بواسطة دالات الـ Hash والنسخ الاحتياطي).
- **التوافر (Availability):** ضمان وصول المستخدمين المصرح لهم إلى الأنظمة والبيانات في أي وقت يحتاجونها (بواسطة صيانة الخوادم ومواجهة هجمات الحرمان من الخدمة).

3. العلاقة بين الشبكات والأمن السيبراني

لا يمكن فصل الأمن السيبراني عن الشبكات؛ **أمن الشبكات (Network Security)** هو أحد أهم فروع الأمن السيبراني. إذا كانت الشبكة هي الطرق والجسور التي تتحرك عليها البيانات، فإن الأمن السيبراني هو نقاط التفتيش، الحراس، وأنظمة المراقبة التي تحمي هذه الطرق.

أبرز آليات حماية الشبكات:

- **جدران الحماية (Firewalls):** أنظمة تصفي حركة المرور الصادرة والواردة بناءً على قواعد أمنية محددة.
- **أنظمة كشف ومنع الاختراق (IDS/IPS):** برمجيات تراقب سلوك الشبكة

لرصد أي نشاط مشبوه أو هجوم ومحاولة إيقافه فوراً.

- **الشبكات الافتراضية الخاصة (VPN):** إنشاء نفق مشفر وآمن لنقل البيانات عبر شبكة إنترنت غير آمنة.

4. أشهر التهديدات والثغرات السيبرانية

تواجه الشبكات باستمرار هجمات متنوعة تهدف إلى سرقة البيانات أو تدمير الأنظمة، ومن أبرزها:

نوع الهجوم	الوصف	وطرق الوقاية
البرمجيات الخبيثة (Malware)	تشمل الفيروسات، برامج الفدية (Ransomware)، وبرامج التجسس.	استخدام مضادات الفيروسات وتحديث الأنظمة دورياً.
التصيد الاحتيالي (Phishing)	رسائل بريد إلكتروني أو روابط مزيفة تخدع المستخدم لسرقة بياناته.	نشر الوعي الأمني وفحص الروابط بدقة.
هجمات حجب الخدمة (DDoS)	إغراق الخادم بحركة مرور هائلة من أجهزة متعددة لإسقاطه وتعطيله.	استخدام خدمات تصفية المرور السحابية وجدران الحماية المتقدمة.
هجوم الرجل في المنتصف (MitM)	اعتراض المهاجم للاتصال بين طرفين للتجسس على البيانات المرسلة.	استخدام بروتوكولات التشفير القوية مثل HTTPS.

5. التوجهات الحديثة في مجال الشبكات والأمن السيبراني

تتطور التكنولوجيا سريعاً، مما يفرض ظهور تقنيات جديدة لمواجهة التهديدات المتطورة:

- **نموذج الثقة الصفرية (Zero Trust Architecture):** مفهوم أمني حديث يقوم على مبدأ **"لا تثق بأحد أبداً، وتحقق دائماً"**. لا يتم الوثوق بأي جهاز أو مستخدم تلقائياً حتى لو كان داخل الشبكة المحلية.
- **الذكاء الاصطناعي في الأمن السيبراني:** استخدام خوارزميات التعلم الآلي لتحليل سلوك الشبكة والتنبؤ بالهجمات وكشف الثغرات قبل استغلالها.
- **أمن الحوسبة السحابية (Cloud Security):** مع انتقال الشركات إلى السحاب (مثل AWS و Azure)، أصبح التركيز ينصب على حماية البيانات الموزعة خارج الحدود الجغرافية التقليدية للشركات.

خلاصة:

إن بناء شبكة قوية وسريعة لم يعد كافياً في العصر الرقمي الحالي ما لم تكن محصنة بـأمن سيبراني متكامل. التحدي الأكبر اليوم ليس فقط في صد الهجمات، بل في القدرة على الاستجابة السريعة والتعافي من الاختراقات بأقل الخسائر الممكنة.

لتطبيق هذا البحث بشكل عملي ومحاكاة بيئة واقعية للشبكات والأمن السيبراني، يمكن تقسيم الخطة العملية إلى **أربعة مراحل أساسية** تنتقل بك من بناء الشبكة وإعدادها، إلى مرحلة الهجوم (لاكتشاف الثغرات)، ثم الدفاع والتأمين، وأخيراً المراقبة والتحليل.

إليك خطة عمل تطبيقية وممنهجة للجانب العملي:

المرحلة الأولى: بناء وتصميم الشبكة (Network Design & Configuration)

الهدف في هذه المرحلة هو فهم كيفية ربط الأجهزة وتوجيه البيانات والتحكم في صلاحيات الوصول.

- **أداة المحاكاة المقترحة:** **Cisco Packet Tracer** (للمبتدئين) أو **GNS3 / Eve-NG** (للمستويات المتقدمة).
- **الخطوات العملية:**

١ **تصميم الهيكلية (Topology):** قم بإنشاء شبكة تضم موجه (Router)، ومبدلين (Switches)، ومجموعة من الأجهزة (PCs, Servers).

٢ **توزيع العناوين (IP Addressing):** قم بتوزيع عناوين IPv4 على الأجهزة بشكل ثابت (Static) وثم إعداد خادم **DHCP** لتوزيع العناوين تلقائياً.

٣ **تقسيم الشبكة (VLANs):** قم بتقسيم الشبكة المحلية إلى شبكات افتراضية (مثلاً: VLAN 10 للموظفين، VLAN 20 للإدارة) لعزل حركة المرور وتحسين الأمن.

٤ **التحكم بالوصول (ACLs):** قم بكتابة قواعد (Access Control Lists) على الموجه لمنع أجهزة "VLAN الموظفين" من الدخول إلى

المرحلة الثانية: بيئة المخترق الأخلاقي (Ethical Hacking Lab)

لفهم الأمن السيبراني، يجب أن تتعلم كيف يفكر المهاجم. في هذه المرحلة يتم إنشاء مختبر اختراق وهمي ومعزول تماماً داخل جهازك (لا تجرب هذا على شبكات حقيقية بدون إذن).

- **الأدوات المقترحة:VirtualBox** أو **VMware** لإنشاء الأنظمة الوهمية.
- **الأنظمة المطلوبة:**
  - **Kali Linux:** نظام التشغيل المخصص للاختراق والأمن السيبراني (يمثل جهاز المهاجم).
  - **Metasploitable / Windows 7 (بدون تحديثات):** أنظمة وهمية تحتوي على ثغرات عمداً (تمثل الضحية).
- **الخطوات العملية:**

١. **جمع المعلومات وفحص الشبكة:** استخدم أداة **Nmap** عبر الـ Kali Linux لفحص نظام الضحية ومعرفة المنافذ المفتوحة (Open Ports) والخدمات الشغالة.

٢. **استغلال الثغرات (Exploitation):** استخدم إطار عمل **Metasploit** للبحث عن ثغرة في أحد المنافذ المفتوحة لدى الضحية واختراق النظام للحصول على صلاحيات التحكم (Shell Access).

المرحلة الثالثة: الدفاع والتأمين (Network Defense & Hardening)

بعد رؤية كيف يمكن اختراق النظام، يأتي دور تطبيق الآليات الدفاعية لحماية الشبكة والبيانات.

- **الأدوات والخطوات العملية:**

١ **إعداد جدار الحماية (Firewall):** قم بتنزيل نظام جدار حماية مفتوح المصدر مثل **pfSense** كنظام وهمي، وقم بإعداد قواعد صارمة تمنع أي حركة مرور غير معروفة من الدخول أو الخروج.

٢ **تشفير الاتصالات:** قم بإعداد بروتوكول **SSH** للتحكم بالأجهزة عن بُعد بدلاً من بروتوكول **Telnet** (لأن Telnet يرسل كلمات المرور بنص واضح غير مشفر ويمكن سرقتها بسهولة).

٣ **تأمين الـ Wi-Fi:** قم بالدخول إلى إعدادات جهاز الراوتر المنزلي وتأكد من تفعيل تشفير **WPA3** (أو WPA2 كحد أدنى) وإغلاق خاصية **WPS** التي تسهل اختراق الشبكة اللاسلكية.

المرحلة الرابعة: المراقبة والتحليل (Monitoring & Analysis)

الأمن السيبراني لا يتوقف عند وضع الحواجز، بل يتطلب مراقبة مستمرة لكشف أي سلوك مريب.

- **الأدوات المقترحة:Wireshark** (لتحليل الحزم) و **Snort** (كنظام كشف اختراق IDS).
- **الخطوات العملية:**

١ **تحليل حركة المرور:** قم بتشغيل برنامج **Wireshark** واجعل جهازك يرسل بيانات (مثل تصفح موقع أو تسجيل دخول). راقب الحزم

(Packets) وكيف تظهر البيانات المشفرة (HTTPS) مقارنة بالبيانات غير المشفرة (HTTP).

٢ **تنصيب نظام كشف الاختراق (IDS):** قم بإعداد **Snort** على الشبكة واكتب قاعدة بسيطة تطلق إنذاراً (Alert) إذا قام أي جهاز بعمل فحص منافذ (Ping Sweep) على الشبكة، لتكتشف إذا كان هناك مهاجم يجمع معلومات.

جدول ملخص للأدوات والمهارات المستهدفة:

المهارة المكتسبة	الأداة الرئيسية	المرحلة
هندسة الشبكات، Routing, Switching, VLANs	Cisco Packet Tracer	**1. بناء الشبكة**
فهم أساليب الاختراق، فحص الثغرات (Penetration Testing)	Kali Linux + Nmap	**2. الهجوم التجريبي**
إدارة جدران الحماية، التشفير، سد الثغرات (Hardening)	pfSense / SSH	**3. الدفاع والتأمين**
تحليل بروتوكولات الشبكة، كشف التهديدات الرقمية	Wireshark	**4. المراقبة والتحليل**

بناء شبكة حاسوبية من الصفر (سواء كانت وهمية للمختبر أو حقيقية) يتطلب السير في خطوات مرتبة لضمان عملها بشكل صحيح وآمن.

سنقوم هنا بشرح **الخطوات العملية لبناء شبكة محاكية داخل برنامج Cisco Packet Tracer** (وهو البرنامج الأسهل والأفضل للبدء عملياً).

الخطوة 1: تصميم الهيكلية الفيزيائية (Topology)

افتح برنامج Packet Tracer وقم بسحب وإسقاط الأجهزة التالية في مساحة العمل:

١. **الموجه (Router):** اختر راوتر (مثل Router 2911) ليربط بين الشبكات المختلفة.
٢. **المبدل (Switch):** اختر مبدلين (مثل Switch 2960)، كل مبدل سيمثل شبكة فرعية أو قسماً مستقلاً.
٣. **أجهزة المستخدمين (End Devices):** اسحب جهازي كمبيوتر (PC) أو لابتوب لكل مبدل.
٤. **التوصيل (Connections):** استخدم الكابل النحاسي المستقيم (Copper Straight-Through) للتوصيل:
   - من الأجهزة (PC) إلى المبدل (Switch).
   - من المبدل (Switch) إلى منفذ الـ Router (مثلاً: منفذ GigabitEthernet 0/0 للشبكة الأولى، ومنفذ GigabitEthernet 0/1 للشبكة الثانية).

الخطوة 2: التخطيط لعناوين الشبكة (IP Planning)

قبل البرمجة، يجب تحديد العناوين التي سنستخدمها لمنع التداخل:

- **الشبكة الأولى (مثلاً: قسم المبيعات):** سنعطيها النطاق 192.168.1.0/24
  - عنوان منفذ الراوتر (المنفذ الافتراضي - Gateway): 192.168.1.1
  - الأجهزة: 192.168.1.2 و 192.168.1.3
- **الشبكة الثانية (مثلاً: قسم الإدارة):** سنعطيها النطاق 192.168.2.0/24
  - عنوان منفذ الراوتر (Gateway): 192.168.2.1
  - الأجهزة: 192.168.2.2 و 192.168.2.3

الخطوة 3: إعداد أجهزة المستخدمين (PCs Configuration)

اضغط على كل جهاز كمبيوتر داخل البرنامج، ثم اذهب إلى تبويب **Desktop** ثم **IP Configuration** وأدخل البيانات كالتالي:

- **للجهاز الأول في الشبكة الأولى:**
  - IPv4 Address: 192.168.1.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.1.1 *(هذا العنوان ضروري لكي يستطيع الجهاز الخروج لشبكات أخرى)*

(كرر نفس العملية لبقية الأجهزة مع تغيير الـ IP حسب التخطيط في الخطوة 2).

الخطوة 4: برمجة الموجه (Router Configuration) عبر السطر البرمجي (CLI)

اضغط على الراوتر، واذهب إلى تبويب **CLI** (واجهة السطر البرمجي)، وابدأ بإدخال الأوامر التالية لتفعيل المنافذ وإعطائها عناوين:

الدخول إلى النمط المميز لنظام سيسكو

```
Router> enable
```

الدخول إلى نمط الإعدادات العام

```
Router# configure terminal
```

الدخول إلى المنفذ الأول المربوط بالشبكة الأولى

```
Router(config)# interface GigabitEthernet 0/0
```

تعيين عنوان IP وقناع الشبكة للمنفذ

```
Router(config-if)# ip address 192.168.1.1 255.255.255.0
```

تشغيل المنفذ (ستتحول الإشارة من الأحمر إلى الأخضر)

```
Router(config-if)# no shutdown
Router(config-if)# exit
```

الدخول إلى المنفذ الثاني المربوط بالشبكة الثانية

```
Router(config)# interface GigabitEthernet 0/1
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

الخطوة 5: فحص الاتصال (Testing Connectivity)

للتأكد من أن الشبكة تعمل بشكل صحيح وأن الراوتر يقوم بتوجيه البيانات بين الشبكتين بنجاح:

١ اضغط على الجهاز الأول 192.168.1.2.
٢ اذهب إلى **Desktop** ثم افتح **Command Prompt** (موجه الأوامر).
٣ اكتب أمر الفحص (Ping) باتجاه جهاز في الشبكة الثانية:

```
ping 192.168.2.2
```

إذا ظهرت لك رسائل تبدأ بـ Reply from... فهذا يعني أن **شبكتك تم بناؤها بنجاح** والبيانات تنتقل بين الأقسام.

تأمين هذه الشبكة

الآن بعد أن قمنا ببناء الهيكل الأساسي للشبكة وجعلنا الأجهزة تتصل ببعضها، سننتقل إلى **الجانب الأمني (تأمين الشبكة)**.
في بيئات العمل الواقعية، لا يُسمح لجميع الأقسام بالوصول إلى بعضها بحرية؛ فمثلاً، يجب منع قسم المبيعات من الدخول إلى خوادم قسم الإدارة أو الموارد

البشرية لأسباب أمنية.

لتأمين هذه الشبكة، سنطبق خطوتين أساسيتين: **منع الوصول غير المصرح به (ACL)**، و**تشفير التحكم عن بُعد (SSH)**.

الخطوة 1: منع الوصول باستخدام قوائم التحكم بالوصول (Access Control Lists - ACL)

سندمج هنا دور جدار الحماية (Firewall) داخل الموجه. نريد **منع** الجهاز 192.168.1.2 (في شبكة المبيعات) من الوصول إلى الشبكة الثانية 192.168.2.0 (شبكة الإدارة)، مع السماح لبقية الأجهزة بالمرور بشكل طبيعي.

اضغط على **الراوتر** وافتح واجهة **CLI**، ثم أدخل الأوامر التالية:

الدخول إلى نمط الإعدادات

Router> enable

Router# configure terminal

إنشاء قائمة تحكم ممتدة (Extended ACL) برقم 101

الأمر أدناه يمنع بروتوكول الـ IP من الجهاز المحدد إلى الشبكة المستهدفة

Router(config)# access-list 101 deny ip host 192.168.1.2 192.168.2.0 0.0.0.255

السماح لجميع الأجهزة والشبكات الأخرى بالمرور دون قيود

Router(config)# access-list 101 permit ip any any

الآن يجب تطبيق هذه القائمة على المنفذ المواجه للشبكة الأولى

Router(config)# interface GigabitEthernet 0/0
Router(config-if)# ip access-group 101 in
Router(config-if)# exit

فحص النتيجة (Testing):

اذهب إلى الجهاز الممنوع 192.168.1.2 وافتح الـ Command Prompt وحاول عمل ping 192.168.2.2. ستلاحظ ظهور رسالة:
Destination host unreachable (أي تم حظر الاتصال بنجاح من قِبل الراوتر).

الخطوة 2: تأمين إدارة الراوتر عبر بروتوكول SSH المشفر

في الشبكات، يقوم المهندس بالتحكم في الراوتر عن بُعد. استخدام بروتوكول **Telnet** القديم يعرض الشبكة لخطر التجسس (MitM) لأن كلمة المرور تُرسل بنص واضح. البديل الآمن هو تفعيل **SSH** الذي يقوم بتشفير كل البيانات المتبادلة.

أدخل الأوامر التالية في **الراوتر** لتشغيل الـ SSH:

1. تعيين اسم للراوتر واسم النطاق (ضروري لتوليد مفاتيح التشفير)

```
Router(config)# hostname SecureRouter
SecureRouter(config)# ip domain-name mynetwork.local
```

2. توليد مفاتيح التشفير (Crypto Keys) وقوتها 1024 بت

```
SecureRouter(config)# crypto key generate rsa
```

(سيطلب منك البرنامج تحديد القوة، اكتب 1024 واضغط Enter)

3. إنشاء حساب مستخدم وكلمة مرور للمهندس بصلاحيات كاملة (Privilege 15)

```
SecureRouter(config)# username admin privilege 15 secret SuperPassword123
```

4. إعداد خطوط الاتصال الافتراضية (VTY) لاستقبال الـ SSH فقط ومنع الـ Telnet

```
SecureRouter(config)# line vty 0 4
SecureRouter(config-line)# transport input ssh
SecureRouter(config-line)# login local
SecureRouter(config-line)# exit
```

فحص النتيجة (Testing):

اذهب إلى أي جهاز كمبيوتر مسموح له بالاتصال في الشبكة، وافتح الـ Command Prompt واكتب الأمر التالي للاتصال بالراوتر بأمان:

ssh -l admin 192.168.1.1

سيطلب منك نظام سيسكو إدخال كلمة المرور (SuperPassword123)، وبمجرد إدخالها ستدخل إلى إعدادات الراوتر بشكل مشفر وآمن تماماً.
بذلك تكون قد قمت ببناء شبكة، وتوجيه البيانات فيها، وحمايتها بقواعد جدار حماية أساسية، وتأمين إدارتها ضد التجسس.

المرحلة التالية ورؤية كيف يمكن لمحلل الأمن السيبراني مراقبة هذه الحزم واكتشاف الثغرات باستخدام أدوات مثل **Wireshark**؟

تحليل ومراقبة الشبكة هو الدور الأساسي الذي يقوم فيه محلل الأمن السيبراني (أو المهندس في مراكز العمليات الأمنية SOC). الأداة الأقوى والأشهر عالمياً في هذا المجال هي **Wireshark** (محلل حزم الشبكة - Packet Analyzer).
في هذه المرحلة، سننتقل من برنامج المحاكاة إلى فهم كيف يرى محلل الأمن البيانات وهي تتحرك في الأسلاك، وكيف يكشف المخاطر.

1. كيف يعمل برنامج Wireshark؟

عند تشغيل Wireshark على جهازك، فإنه يضع بطاقة الشبكة في وضع يُسمى **Promiscuous Mode**، وهو ما يتيح لها "الاستماع" والتقاط (Capture) لجميع الحزم والبيانات التي تمر عبر الشبكة، سواء كانت متجهة لجهازك أو لأجهزة أخرى.
يقوم البرنامج بتقسيم واجهته إلى ثلاثة أقسام رئيسية:

١. **قائمة الحزم (Packet List):** تعرض جميع الحزم الملتقطة مع الوقت، المصدر (Source IP)، الوجهة (Destination IP)، ونوع البروتوكول.
٢. **تفاصيل الحزمة (Packet Details):** تفكيك الحزمة المحددة بناءً على طبقات نموذج OSI (التي ذكرناها في أول البحث).
٣. **عرض البيانات بالبايت (Packet Bytes):** عرض البيانات شكلها الخام (Hexadecimal والنص المقابل لها).

2. سيناريو عملي: كشف سرقة كلمة المرور (Telnet vs SSH)

دعنا نرى كيف يكشف محلل الأمن السيبراني خطورة البروتوكولات غير المشفرة عملياً:

الحالة الأولى: مراقبة اتصال غير مشفر (Telnet)

إذا قام مهندس الشبكة بالاتصال بالراوتر باستخدام بروتوكول Telnet القديم لحل مشكلة ما، وقام محلل الأمن (أو المخترق) بتشغيل Wireshark في نفس الوقت:

١ سيقوم المحلل بفلترة الحزم بكتابة telnet في شريط البحث.
٢ بالضغط بالزر الأيمن على إحدى الحزم واختيار **Follow TCP Stream** (متابعة دفق البيانات)، ستظهر نافذة تعرض كل ما حدث في الجلسة.
٣ **النتيجة الصادمة:** ستظهر كلمة المرور واسم المستخدم مكتوبة بنص واضح تماماً (Plain Text) كما أُرسلت، وبالتالي يمكن لأي شخص على الشبكة سرقتها فوراً.

الحالة الثانية: مراقبة اتصال مشفر (SSH)

إذا قام المهندس بتطبيق الخطوة الأمنية التي فعلناها سابقاً وتحول إلى SSH:

١ عند فحص الحزم في Wireshark وكتابة فلتر ssh.
٢ عند محاولة عمل **Follow TCP Stream** لقراءة البيانات.
٣ **النتيجة الأمنية:** ستظهر البيانات على شكل رموز عشوائية ونصوص غير مفهومة (Encrypted Data). حتى لو نجح المهاجم في اعتراض الحزمة، فلن يستفيد منها شيئاً لأنها مشفرة بمفاتيح رياضية معقدة.

3. كشف الهجمات عبر تحليل الحزم

محلل الأمن السيبراني يستخدم Wireshark أيضاً لاكتشاف إذا كانت الشبكة تتعرض لهجوم في الوقت الفعلي. إليك مثالين:

- **كشف فحص المنافذ (Nmap Ping Scan):** إذا وجد المحلل في قائمة الحزم أن هناك جهازاً واحداً (مثلاً 192.168.1.5) يرسل آلاف الحزم من نوع SYN إلى أجهزة مختلفة في الشبكة خلال ثوانٍ معدودة، يعلم فوراً

أن هذا الجهاز يقوم بعملية **Reconnaissance** (جمع معلومات ومسح للشبكة) للتحضير لهجوم، فيقوم بحظره فوراً عبر جدار الحماية.

- **كشف هجوم حجب الخدمة (DDoS):** إذا غصت الشاشة بحزم ضخمة ومتتالية من نوع UDP أو ICMP قادمة من مصادر خارجية باتجاه خادم الموقع الإلكتروني، يدرك المحلل أن هناك محاولة لإغراق الخادم وإسقاطه، فيفعل خطط الطوارئ وتصفية المرور.

بهذه الخطوة التطبيقية، نكون قد أغلقنا الدائرة الكاملة للبحث: **بنينا الشبكة**، **فهمنا ثغراتها**، **قمنا بتأمينها**، و**تعلمنا كيف نراقبها ونحلل حركتها**.

خلاصة الجانب العملي

تثبت هذه الدراسة التطبيقية أن أمن المعلومات ليس منتجاً ثابتاً يشترى بل هو عملية مستمرة وممنهجة. يبدأ الأمن من التصميم الفيزيائي الصحيح للشبكة، ومروراً بسد الثغرات وتشفير القنوات، وصولاً إلى المراقبة المستمرة والتحليل اللحظي لحركة البيانات لضمان ديمومة مثلث الأمن السيبراني (السرية، السلامة، والتوافر).

By:Haytham Zeidan

https://archive.org/details/@wazefapress